DOCUMENT ID: 2PAA121221
REVISION: C
DATE: 2020-04-17

CYBERSECURITY ADVISORY

SECURITY System 800xA Weak Registry Permissions

CVE ID: CVE-2020-8474

Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by ABB.

ABB provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall ABB or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if ABB or its suppliers have been advised of the possibility of such damages.

Affected products

System 800xA Base versions 6.0 and earlier

Vulnerability ID, Product Issue Number

CVE ID	Product Issue Number
CVE-2020-8474	800xASYS-OL-5120-00197

Summary

An update is available that resolves a privately reported vulnerability in the product versions listed above.

Low privileged users are allowed to read, modify, add and delete registry settings that are used to control system functionality. An authenticated attacker who successfully exploited this vulnerability could cause system functions to stop or to misbehave.

Vulnerability severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3. The CVSS Environmental Score, which can affect the vulnerability severity, is not provided in this advisory since it reflects the potential impact of a vulnerability within the end-user organizations' computing environment; end-user organizations are therefore recommended to analyze their situation and specify the Environmental Score.

CVSS v3 Base Score: 7.8 (High)

CVSS v3 Temporal Score: 7.5 (High)

CVSS v3 Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C

CVSS v3 Link : https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C

NVD Summary Link: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-8474

Recommended immediate actions

ABB recommends changing any user account passwords which are suspected to be known by an unauthorized person. Interactive logon (both local and remote) is recommended to be disabled for the service account.

The vulnerability is corrected in System 800xA Base 6.1. The vulnerability is planned to be corrected in the next release on the 6.0.3 LTS track after 6.0.3.3.

Please note that the vulnerability can only be exploited by authenticated users, so customers are recommended to ensure that only authorized persons have access to user accounts in System 800xA.

Vulnerability details

Access control settings for parts of the Windows registry handled by System 800xA, allow low privileged users to read, modify, add or delete content used by system functions.

An authenticated attacker who successfully exploited the vulnerabilities could cause different systems to malfunction.

Mitigating factors

As described above, the mitigating factor is that an attacker needs to be able to login to an account in the system, so the primary mitigation is to ensure that only authorized persons have access to user accounts on the system nodes. This also includes any user accounts accessing the system via remote tools like Remote Desktop.

More information on recommended practices can be found in section References.

Workarounds

There are no workarounds for this vulnerability, only mitigating actions. The products require an update to fully remedy the vulnerability.

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could escalate his/her privileges, cause system functions to stop or malfunction.

What causes the vulnerability?

The vulnerability is caused by weak access control lists for registry settings allowing low privileged users to modify system settings.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could escalate his/her privileges, cause the affected system node to stop or become inaccessible.

Can functional safety be affected by an exploit of this vulnerability?

No, exploits of this vulnerability cannot affect the integrity of any safety function in System 800xA.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by logging in to an 800xA node and modify the registry in such a way that the system will load access malicious code, which will be executed as part of the system.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access and access to an account that can login to the system node remotely could exploit this vulnerability. Recommended practices include that process control systems are physically protected, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed. See *Mitigating factors*.

What does the update do?

The update removes the vulnerability by ensuring that the access control list limits access for the registry information.

When this security advisory was issued, had this vulnerability been publicly disclosed?

No, ABB received information about this vulnerability through responsible disclosure.

When this security advisory was issued, had ABB received any reports that this vulnerability was being exploited?

No, ABB had not received any information indicating that this vulnerability had been exploited when this security advisory was originally issued.

Acknowledgement

ABB thanks William Knowles at Applied Risk for helping to identify the vulnerabilities and protecting our customers.

References

3BSE080520* System 800xA, Security Deployment Guide.

3BSE041389* 800xA System, Engineering Planning and Concepts.

3BSE034463* System 800xA Network Configuration.

Support

For additional instructions and support please contact your local ABB service organization. For contact information, see www.abb.com/contactcenters.

Information about ABB's cybersecurity program and capabilities can be found at www.abb.com/cybersecurity.

Revision

Rev.	Page (P) Chapt. (C)	Description	Date
A	all	New document	2020-03-04
B	P2	Clarified section Recommended immediate actions	2020-03-26
C	P3 all	Added FAQ question on functional safety Misc clarifications	2020-04-17